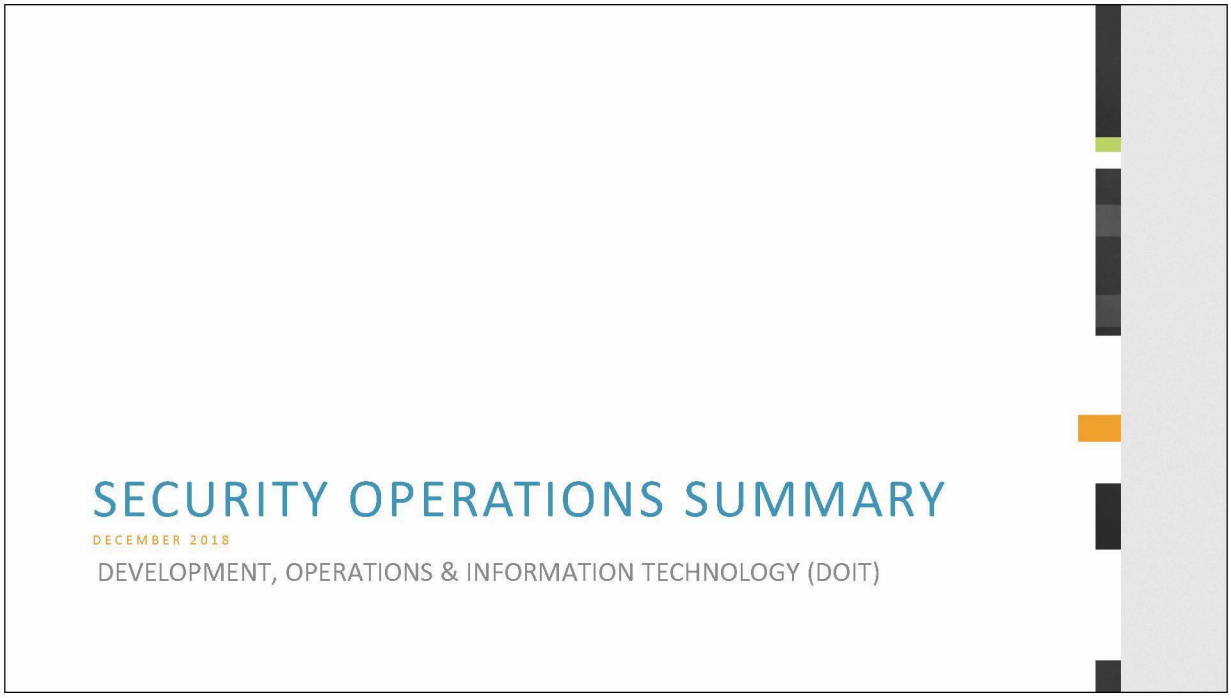
Exhibit 20

Excerpts of SW-SEC00638663


SECURITY OPERATIONS SUMMARY
DECEMBER 2018
DEVELOPMENT, OPERATIONS & INFORMATION TECHNOLOGY (DOIT)

SECURITY PROJECTS
KEY AREAS TO ADDRESS GAPS IN INFORMATION SECURITY

solarwinds

CSF Mapping	Focus Area	Gap Analysis
Identify	Mobile Device Management (MDM)	Enable and manage employee mobile devices for remote access to the corporate network
	Security Assessment and Remediation	Conduct an enterprise-wide security assessment using the NIST Cybersecurity framework
	Security Standards and Governance	Develop a set of security standards and guidance documentation that aligns with our adoption of the NIST Cybersecurity framework
	Security Awareness Training	Establish a formal program to educate users on the importance of protecting SolarWinds information and information systems
	Enterprise Access Management (Standard and Audits)	Define standards and best practices for Role Based Access Controls and Least Privilege
	Security & SSDLC	Integrate and formalize security best practices into existing secure development lifecycle
Protect	Phishing as a Service	Education and training program to raise awareness and understand potential impact to individual and the company
	Privilege Access Management (PAM) and Multifactor Authentication	Address the use of local administrator access to non-privileged users. Manage, audit, and apply security controls around privileged access.
	Data Loss Prevention, Cloud Access Security Broker (CASB)	DLP, Management of security controls around cloud based applications, threat intelligence around compromised corporate email
Detect	Product Penetration Testing	No formalized testing, Identify and integrate penetration testing into product development phases
Respond	BCP/ Disaster Recovery Planning	Formalize DRP and exercise on a routine basis
Recover		

Other Items/Notes

solarwinds

- Evaluation of Nexpose vulnerability scanner against OpenVAS (MSP)
- Scheduling After Action Reviews (AAR) to close out MSP incidents
- Security standards and guidelines for use in GDPR corrective action plan (CAP) items.
- Security statements around InfoSec program
  - NDA vs. non-NDA versions for customer inquiries
  - Internet facing security statement for publishing on website
  - GDPR statement (Published)